REMARKS/ARGUMENTS

This application has two independent claims, 1 and 7, as follows (emphasis added):

> 1. External signing device for a PC with an optical data input via the monitor, characterized in that said device includes an optical system for receiving the data from a computer monitor, an alphanumerical display for showing the data to be signed, a keyboard for user interaction with the device and a signing system to process the operations of signing the data received.
>
> 7. An external digital signing device, said device comprising:
> a display, wherein said display displays output received from a computer;
> an optical system, wherein said optical system receives said output from said display;
> a keyboard, wherein said keyboard receives input from a user, and transmits said user input to said device; and
> a signing system, wherein said signing system processes operations directed to digitally signing said output received from said display.

These features correspond in the disclosed embodiment to the signing device (1,2,3,4) shown in Fig. 1, which has photodetectors (5) for receiving data from a display on a computer monitor (6).

All of claims 1-19 are believed patentable over the art, taken individually or in combination, and all issues are reserved for purposes of appeal.

Claims 1, 3, 5, 7, 10-13 and 15-18 including both of the independent claims have been rejected as anticipated by Houvener. The rejection is respectfully traversed.

The Examiner states that Houvener has "an optical system (terminal 1) for receiving the data from a computer monitor (input device 9) (col. 4, lines 45-65)".

Col. 4, lines 45-65, reads as follows:

> "A point of identification terminal 1 is located at a location where the identity of persons present is required to be verified. The point of identification terminal comprises a standard magnetic strip

reader 4, an optional bar code reader 4', a check scanner 4" (all of which are well known in the art), an optional input 5 (which may be a numeric keypad, an alpha-numeric keypad or simply a series of a few dedicated keys), a display means 6, which is preferably a miniature flat panel display, a controller 7, and an internal communication modem or other communication means 8. Also included, as either an integral component of the point of identification terminal or as a separate component, is a biometric input device 9. In one preferred embodiment, the biometric input device comprises a fingerprint scanner for scanning fingerprints of system users to authenticate their authority to access and use the system. However, other biometric input devices, configured to read other biometric data, such as retinal scans, voiceprints, thermal images and the like may work equally well and are envisioned within the scope of the present invention.

One fingerprint scanner, which was recently announced..."

It cannot be more plain that the input device 9 is a biometric device such as a fingerprint scanner and is not an optical system that receives or is capable of receiving data from a computer monitor display.

The Examiner mentions that Houvener discloses additional input devices, such as bar code readers, check scanners, and alternative types of biometric devices. But again, none of these is an optical system that receives or is capable of receiving data from a computer monitor display.

Thus, contrary to the Office Action, Houvener simply does not have "an optical system (terminal 1) for receiving the data from a computer monitor (input device 9) (col. 4, lines 45-65)". The Examiner has not pointed out any optical device in Houvener receiving data from a computer display. The anticipation rejection of claims 1, 3, 5, 7, 10-13 and 15-18 should therefore be withdrawn.

Claims 4, 6, 11, 14 and 19 have been rejected over Houvener in view of Drummond et al. Claims 2 and 8-9 have been rejected over Houvener in view of Hacker et al. These issues have been adequately discussed in the Amendment dated May 15, 2006, incorporated by reference, and discussed further hereinbelow. Claims 2, 4, 6, 8-9, 11, 14 and 19 should be allowed.

The background, the technical field and some salient characteristics of the invention will now be discussed.

Houvener's US patent 6,424,249 relates to a system for identification of a user which is associated with the stage prior to a monetary transaction. The present invention relates to a digital signature system for operations which guarantees to the user the integrity of the data to be signed and which is associated with the authorisation step, as part of the bank transaction itself.

The invention of claims 1 and 7 provides an optical communications system for receiving data from a computer monitor, with no need for any physical cable connection. According to various claims, the identity of the user is proved by the possession of the signature keys which are only known by the device (stored internally and thereby protected) and by the validation authority in charge of verifying the authenticity of the signature provided.

The claimed signature device may be a personal device which may be carried by the person and used anywhere and with any computer, optically, while Houvener's device is a terminal which would be available in commercial establishments, cable-connected to a computer, as a complement of the point of sale terminal (PST) and whose identification system is based on the inclusion of a biometric identification device.

Houvener's identification device is comprised of a terminal (1) which includes:

- A magnetic strip reader (for example, for credit cards) and optionally, a bar-code reader.

- A data entering device (for example, an alphanumeric keypad).
- A means of display (for example, a flat panel).
- A controller.
- A means of communication (for example, a modem and cable).
- A biometric data entry device (for example, by scanning of the retina, fingerprint, voice or thermal image).

Houvener's identification device appears to operate as follows:

- A biometric datum of the user to be identified is entered, through the biometric data entry device.
- The biometric datum obtained is transmitted from the identification device to a remote database (for example, via the modem and cable).
- The biometric data received are compared with the models stored in the remote system.
- If identification is correct, the user must enter, by means of the data entering device, the data requested by the identification device.
- The remote system sends photographic data corresponding to the user, which will appear on the means of display of the identification device, so that the salesperson may verify the identity of the user. The photographic data may comprise an image of the physical appearance of the person or his/her signature.

The device of claims 1 and 7 is a digital signature device which may be similar to a smart card and which incorporates the user's signature key.

This type of card is generally of a small size, carried by the user and not by the vendor; that is to say, on arriving at the point of sale, the user uses his/her own smart card as a means of identification. It is therefore not the vendor's device.

Thus, for example, in the section of "Background of the Invention" (last three paragraphs) the operation and problems of smart cards are described, and the first paragraph of the "Description of the Invention" says that: "the system associated with the device disclosed herein extends the functionality of smart cards", that is, related or referring to smart cards carried by the user and not to means of identification provided by the vendor.

In any case, the device of the present claims is completely different from that mentioned in Houvener's patent, both in its components and in its operation.

The external signature device of claims 1 and 7 and other claims may be comprised of the following elements:

- An optical system for receiving data from a computer monitor (2). By means of this optical system, the data to be signed are received, not user identification data. Moreover, these data are received by optical means from the monitor of the vendor's computer. To do this, the external signature device (smart card) is placed facing the computer monitor in order to receive (optically) the data to be signed. This may be clearly seen in figure 1.
- A VDU or alphanumeric display panel, for the displaying of the data to be signed (received via the optical system).
- A keypad for communication of the user with the device (entering of data and keys).
- A signature system, responsible for processing the operations of signing the data received (generation of the electronic signature code).

The system of claims 1 and 7 exhibits many characteristics distinguishing it from previous smart cards and from the cited prior art, including:

- A system for displaying the data to be signed by the user before signing. This prevents the user from signing undesired data. These data are displayed on the external signature device, which is the property of the user and, not being re-programmable, it is immune to software attacks which might alter the behavior of the same with the goal of achieving the user's signature authorizing data different from those desired (which will be shown on the display of the device prior to signature).
- The transmission of the data to be signed from the computer to the external signature device is carried out optically. Connecting cables are not needed. Data transmission is carried out by optical means which cannot be interfered with by third parties. This transmission is carried out from the computer monitor to the external signature device. This makes it possible to use the system with any type of computer (via its monitor), requiring no type of installation or special configuration.

The claimed device is different from that disclosed in the Houvener patent for at least the following reasons:

- It is an external signature device (smart card), that is, a digital signature device which therefore is a portable piece of equipment which is the property of the user, who uses and activates the same when he/she is going to carry out a commercial transaction. The Houvener device is a user identification device which is the property of the vendor.
- The claimed device incorporates a system for the transmission of the data to be signed from the vendor's computer to the user's smart card. This transmission is carried out between the

computer monitor and the smart card by optical means. Houvener's only "optical" device is a scanner which obtains biometric data from the body of the client for the identification of the client. There is no disclosure nor any capability of optical data transmission from the computer monitor to the external identification device. As claimed the data are the information to be signed, while in Houvener's patent they are the biometric data of the user.

- The claimed device incorporates a display on which the data to be signed are shown. On Houvener's display, photographs identifying the user (for example, an image of the physical appearance of the user or an image of his/her signature) are displayed.
- In the claimed device, there is no need for data transmission via cables, connectors or modems which might be interfered with or pirated. An optical transmission of data is used. With the device of the various claims, one mode of operation could be as follows:
- The user who is about to carry out a monetary transaction activates his/her own signature device by entering a PIN via the keypad (4).
- Subsequently, he/she places the signature device opposite the vendor's computer monitor (so that the optical data receiving system is facing the monitor) in order to receive the data to be signed. The data are transmitted from the monitor to the optical data receiving system of the signature device.
- The data received by the external signature device are shown on the display (3) so that the user may verify that they are correct.
- If the data are correct, the user will order signature of the same.
- The signature device generates an electronic signature code which appears on the display (3).
- The user enters the signature code into the vendor's computer, by means of the computer

keyboard itself.

In summary, the device of the claims operates differently and is structured differently than the device of the Houvener patent.

The Hacker patent relates to a portable data acquisition terminal of the type commonly used by salespersons or product distributors in order to monitor sales, product stocks and prices. These terminals are comprised of a keypad for the entering of data, a display panel and a connector for connection to a computer for the downloading of data.

The terminal of Hacker's patent incorporates a module (16) which may be coupled to the body of the terminal in order to verify handwritten data (for example, a handwritten signature). This signature verification may be carried out in two ways:

- The module (16) may utilize an optical scanner (20) which can scan the handwritten signature and store it in the memory for verification purposes. It is possible the Examiner is confusing Hacker's optical scanner, which in this case is placed facing a handwritten signature on a writing surface in order to scan the same, with the device of claims 1 and 7, which has an optical device capable of receiving data from a computer monitor, specifically by recognizing color changes in an area of the same.
- The module (16) may comprise some pressure-sensitive resistive layers, so that the signature is executed directly on the screen (20) of the module.

Hacker's solution is obviously different from the device of claims 1 and 7, as it does not incorporate any optical device as claimed.

According to the Examiner, a solution similar to that described in claim 2 may be observed in Hacker, column 7, lines 5 to 45.

The applicant's cannot agree with the examiner. In claim 2, it is mentioned that the computer monitor, for the purpose of data transmission, incorporates two sections (6, 6'), one for the sending of data and the other for synchronism and the optical receiving system is comprised of photodetectors for the detection of signals sent by the monitor.

In the aforementioned paragraph of the Hacker patent there is a description of a bar-code scanner which incorporates a series of illumination photodiodes which simulate an instantaneous flash, in such a way that Hacker's scanner describes the reflected bar-code image. There is suggestion in Hacker's scanner of the monitor of claim 2.

There are several additional inaccuracies in the final Office Action.

- Page 4, point 3. The Examiner says that Houvener's patent incorporates an optical system (input device 9) for receiving data from a computer monitor. This is completely wrong. Device (9) is an input device for the biometric data of the user, that is, data related to characteristics which are specific to the user, such as his/her fingerprints, voice, retina, etc. Besides, these data are not received from a computer monitor. The device (9) only obtains biometric data; it is a scanner.
- Page 4, point 3. The Examiner says that Houvener's patent incorporates an alphanumeric display (6) to display the data to be signed. Neither is this correct: the display (6) allows photographs for the identification of the user to be seen, not the data which correspond to the transaction which is to be signed by the user.
- Page 9, first paragraph. The Examiner says that in Hacker's patent a definite area on the monitor for the transmission of data into the optical detector is described. This is not correct either: nowhere in Hacker's patent is there mention of a computer monitor which sends data

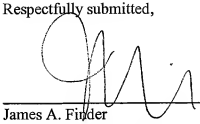
to an optical detector, as claimed.

In view of the foregoing, reconsideration and allowance of claims 1-19 is requested.

THIS CORRESPONDENCE IS BEING SUBMITTED ELECTRONICALLY THROUGH THE PATENT AND TRADEMARK OFFICE EFS FILING SYSTEM ON February 5, 2007.

JAF:lf

Respectfully submitted,



James A. Finder
Registration No.: 30,173
OSTROLENK, FABER, GERB & SOFFEN, LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700